

Atty. Dkt. No. 200301736-2CLAIM AMENDMENTSRECEIVED
CENTRAL FAX CENTER

JAN 24 2007

This listing of claims will replace all prior versions, and listings, of claims in the application.

- 1 1. (Currently Amended) A method for backing up data on a plurality of
2 computers connected via a network, comprising:
3 forming one or more backup partnerships among the plurality of
4 computers such that each computer in a backup partnership commits under an
5 agreement to store backup data received from one or more of its backup partners,
6 whereby a first computer in each partnership assumes the task of storing backup
7 data received from one or more other computers in the partnership and one or
8 more of the other computers in the partnership assume the task of storing backup
9 data received from the first computer;
10 backing up data in accordance with each agreement; and
11 periodically verifying that previously backed up data is being retained by
12 the computers committed to act as backup partners in accordance with each
13 agreement.
- 1 2. (Original) The method of claim 1, further comprising:
2 selecting potential backup partners from among the plurality computers
3 based on predetermined criteria.
- 1 3. (Original) The method of claim 1, further comprising:
2 negotiating the agreements between the plurality of computers based on
3 predetermined requirements, including backup requirements.
- 1 4. (Previously Presented) The method of claim 1, wherein the plurality of
2 computers administer a distributed cooperative backing up of data in the absence
3 of central control.

Atty. Dkt. No. 200301736-2

1 5. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is encoded with an erasure code.

1 6. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is encoded with an error correction code.

1 7. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is encrypted.

1 8. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is encoded with an erasure code and then encrypted, the
3 encoding being for fault tolerance and the encryption being for data security.

1 9. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is compressed and then encoded with an erasure code.

1 10. (Withdrawn) The method of claim 9, wherein the compression is a lossless
2 data compression.

1 11. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the data is, in sequence, compressed, encoded with an erasure code and
3 encrypted.

1 12. (Withdrawn) The method of claim 1, wherein each time before the data is
2 backed up the method further comprises, in sequence:
3 performing data compression;
4 performing a first data encryption;
5 performing encoding with an erasure code; and
6 performing a second data encryption.

Atty. Dkt. No. 200301736-2

1 13. (Withdrawn) The method of claim 12, wherein the first encryption is for
2 data security and the second encryption is for preventing freeloading by any of the
3 backup partners, and wherein the encoding is for fault tolerance.

1 14. (Withdrawn) The method of claim 1, further comprising:
2 restoring data from the previously backed up data.

1 15. (Original) The method of claim 1, wherein each of the plurality of computers
2 has a storage, the storage being periodically scanned to find data to be backed up
3 and identify data previously backed up that no longer needs to be backed up, the
4 data to be backed up being retrieved from the storage for a next periodic backup.

1 16. (Previously Presented) The method of claim 1, wherein the verifying that
2 previously backed up data is retained by the backup partners includes monitoring
3 the backup partners, and for any one of the backup partners being monitored,
4 selecting a block of data stored at the monitored backup partner,
5 requesting the block of data from the monitored backup partner, and
6 receiving from the monitored backup partner and checking the block of
7 data to determine if the block of data represents a corresponding block of
8 previously backed up data.

1 17. (Original) The method of claim 16, wherein the block is selected randomly.

1 18. (Previously Presented) The method of claim 16, wherein the block is selected
2 using a protocol to produce a number that corresponds to the selected block and
3 that is controlled by at least two backup partners.

1 19. (Original) The method of claim 18, wherein the protocol, being performed
2 by any computer of the plurality of computers, includes
3 sending by the computer to a monitored one of its backup partners a hash
4 value of a first random number,

Atty. Dkt. No. 200301736-2

5 receiving by the computer from the monitored one of its backup partners a
6 second random number,
7 sending by the computer to the monitored one of its backup partners the
8 first random number,
9 computing the number from the first and second random numbers by both
10 the computer and the monitored one of its backup partners.

1 20. (Original) The method of claim 1, further comprising:
2 selecting another computer connected via the network to be a new backup
3 partner if it is determined that a backup partner has reneged by not retaining the
4 previously backed up data;
5 negotiating and, if an agreement is reached, forming a partnership with the
6 other computer, accepting the other computer as the new backup partner.

1 21. (Original) The method of claim 20, wherein selecting another computer to be
2 the new backup partner includes
3 determining if there are sufficient backup partners for backing up the data,
4 and
5 searching for the other computer based on predetermined criteria including
6 one or both of geographic separation and system diversity.

1 22. (Original) The method of claim 20, wherein if after accepting the other
2 computer as the new backup partner it is determined that the backup partners are
3 insufficient in number for backing up the data, the selecting, negotiating and
4 forming backup partnership with yet another computer are repeated, the
5 determining, selecting, negotiating and forming backup partnership being
6 repeated until the number of backup partners is sufficient.

1 23. (Original) The method of claim 2, wherein selecting computers as potential
2 backup partners includes

Atty. Dkt. No. 200301736-2

3 determining if there are sufficient backup partners for backing up the data,
4 and
5 searching for computers based on the predetermined criteria that includes
6 one or both of geographic separation and system diversity.

1 24. (Original) The method of claim 3, wherein negotiating the agreements
2 includes, for any computer of the plurality of computers,
3 exchanging queries between the computer and computers selected as its
4 potential backup partners about each such computer's ability to satisfy the
5 predetermined requirements that include one or more of
6 predictable and suitable time schedule for being on-line,
7 suitable network bandwidth,
8 matching backup space requirements, and
9 backup track record.

1 25. (Original) The method of claim 24, wherein, the computer prefers to partner
2 with those of its potential backup partners that satisfy the predetermined
3 requirements.

1 26. (Original) The method of claim 24, wherein the suitable network bandwidth
2 is equal or larger than a predetermined threshold bandwidth and is characterized
3 by an average bandwidth that is larger than the predetermined threshold
4 bandwidth.

1 27. (Original) The method of claim 24, wherein the backup track record includes
2 not reneging on a number of other backup partners that is greater than a
3 predetermined number.

1 28. (Original) The method of claim 1, wherein each of the backup partners has a
2 recent copy of a list of its backup partners' other backup partners.

Atty. Dkt. No. 200301736-2

1 29. (Withdrawn) The method of claim 1, wherein a user of each of the plurality
2 of computers can obtain a copy of a list containing identifiers and/or identities of
3 the backup partners associated therewith and an encryption key under which the
4 data is encrypted prior to being backed up.

1 30. (Previously Presented) The method of claim 1, wherein the agreements are
2 respectively negotiated between the plurality of computers such that in each
3 partnership each computer commits to avoid making or honoring a data
4 restoration request for a commitment period that is longer than a grace period,
5 wherein the grace period for a backup partner of a computer starts to run if it is
6 determined that the backup partner has failed to respond to such computer
7 verifying that the backup partner is retaining the previously backed up data or to
8 prove to such computer that it is retaining the previously backed up data, and
9 wherein upon the grace period running out such computer considers the backup
10 partner to have reneged on its agreement.

1 31. (Withdrawn) The method of claim 7, wherein any encryption algorithm can
2 be suitably used for encrypting the data being backed up, including DES (data
3 encryption standard), RC4, RSA or other public-key encryption.

1 32. (Withdrawn) The method of claim 6, wherein the error correction code is a
2 Reed Solomon code.

1 33. (Withdrawn) The method of claim 5, wherein for a low degree of fault
2 tolerance the erasure code is $n+1$ -parity.

1 34. (Withdrawn) The method of claim 7, wherein after the encryption of the data
2 the encrypted data is divided into blocks and cryptographic checksums or digital
3 signature are added to each block before the blocks are sent each to a particular
4 one of the backup partners.

Atty. Dkt. No. 200301736-2

1 35. (Withdrawn) The method of claim 5, wherein the encoding with the erasure
2 code uses Tornado coding.

1 36. (Withdrawn) The method of claim 5, wherein the encoding with the erasure
2 code includes

3 dividing the data being backed up into blocks, and
4 adding redundancy to each of the blocks producing data objects with
5 actual data portions and redundant data portions, so that each one of the actual
6 data portions and redundant data portions is being backed up at a distinct one of
7 the backup partners.

1 37. (Withdrawn) The method of claim 1, further comprising:
2 dividing the data being backed up into blocks;
3 creating a hash value of each of the blocks using a key; and
4 correspondingly appending the hash values to their blocks before the
5 blocks are each sent to a distinct one of the backup partners.

1 38. (Withdrawn) The method of claim 37, wherein the hash values are later used
2 in periodically verifying that the previously backed up data is retained by the
3 backup partners and, if needed, that the previously backed up data being retained
4 is valid and can be used to restore lost data.

1 39. (Withdrawn) The method of claim 37, wherein the periodic verifying
2 includes
3 selecting and requesting a particular one of the data blocks that was
4 previously backed up,
5 retrieving the particular one of the data blocks and its associate hash value,
6 computing a new hash value from the retrieved particular block using the
7 key, and

Atty. Dkt. No. 200301736-2

8 comparing the new hash value with the associated hash value to determine
9 if they are equal, equality indicating that the data block is retained by the backup
10 partner and is valid.

1 40. (Withdrawn) The method of claim 1, wherein the encoding includes dividing
2 the data being backed up into p groups of m blocks, each of the p groups
3 representing a vector of actual data and the m blocks in each of the p groups
4 representing m elements of the actual data vector; and adding redundancy to each
5 actual data vectors producing p codewords each being a vector of $n=m+k$
6 elements, so that each one of the n elements is being backed up at a distinct one of
7 the backup partners.

1 41. (Withdrawn) The method of claim 14, wherein the restoring of data from the
2 previously backed up data includes
3 retrieving blocks of the previously backed up data from the backup
4 partners until sufficient blocks of the previously backed up data are available for
5 decoding,
6 checking, for each retrieved block of the previously backed up data, if the
7 retrieved block is valid and intact,
8 decoding all the retrieved blocks of the previously backed up data to
9 reconstruct the data originally backed up.

1 42. (Withdrawn) The method of claim 14, wherein the restoring of data from the
2 previously backed up data includes
3 retrieving previously backed up data from the backup partners until
4 sufficient previously backed up data is available for decoding,
5 decoding all the retrieved previously backed up data to reconstruct the
6 data originally backed up, and
7 decrypting the data originally backed up to obtain the actual data.

Atty. Dkt. No. 200301736-2

1 43. (Withdrawn) The method of claim 14, wherein the restoring of data from the
2 previously backed up data includes
3 retrieving previously backed up data from the backup partners until
4 sufficient previously backed up data is available for decoding, and
5 decrypting, decoding and decompressing all of the retrieved previously
6 backed up data.

1 44. (Original) The method of claim 1, wherein the data being backed up is file
2 contents.

1 45. (Currently Amended) A distributed cooperative backup system, comprising:
2 a network; and
3 a loose confederation of computers connected via the network, a plurality
4 of computers from among the loose confederation of computers being configured
5 for distributed cooperative backing up of data, each computer of the plurality of
6 computers having a storage that can be used for providing reciprocal backup
7 services, and each computer of the plurality of computers respectively having a
8 computer readable medium embodying computer program code configured to
9 cause the computer to
10 form backup partnerships between the plurality of computers, each of the
11 backup partnerships being of computers such that each computer in a partnership
12 commits under an agreement to store backup data received from one or more of
13 its backup partners, whereby a first computer in each partnership assumes the task
14 of storing backup data received from one or more other computers in the
15 partnership and one or more of the other computers in the partnership assume the
16 task of storing backup data received from the first computer;
17 back up data in accordance with each agreement; and
18 periodically verify that previously backed up data is being retained by the
19 computers committed to act as backup partners in accordance with each
20 agreement.

Atty. Dkt. No. 200301736-2

1 46. (Previously Presented) The system of claim 45, wherein each of the backup
2 partners is allowed to leave the system and return to the system.

1 47. (Previously Presented) The system of claim 45, wherein prevention of
2 freeloading is enforced by the backup partners, by any of the backup partners
3 being requested to prove that it is retaining the previously backed up data.

1 48. (Previously Presented) A distributed cooperative backup system, comprising:
2 a network; and
3 a loose confederation of computers connected via the network, a plurality
4 of computers from among the loose confederation of computers being configured
5 for distributed cooperative backing up of data and functioning as backup partners,
6 each computer of the plurality of computers having a storage that can be used for
7 providing reciprocal backup services, and each computer of the plurality of
8 computers respectively having a computer readable medium embodying computer
9 program code configured to cause the computer to
10 select computers as potential backup partners from among the plurality of
11 computers based on predetermined criteria,
12 negotiate a reciprocal backup partnership agreement between the computer
13 and the selected computers based on predetermined requirements, including
14 backup requirements,
15 form partnerships between the computer and selected computers, the
16 computer and the selected computers becoming backup partners by agreeing to
17 cooperatively provide backup services to each other such that a first computer in
18 each partnership assumes the task of storing backup data received from one or
19 more other computers in the partnership and one or more of the other computers
20 in the partnership assume the task of storing backup data received from the first
21 computer and so that a distributed cooperative backing up of data is administered
22 in the absence of central control,
23 periodically back up data at the backup partners, encoding the data each
24 time before the data is backed up, and

Atty. Dkt. No. 200301736-2

25 periodically verify that previously backed up data is retained by the
26 backup partners.

1 49. (Previously Presented) A method for backing up data on a plurality of
2 computers connected via a network, comprising:
3 exchanging messages among computers of the plurality to determine the
4 ability of each to satisfy backup storage requirements of one or more others;
5 forming a partnership among computers of the plurality in which a first
6 computer in the partnership stores backup data received from one or more other
7 computers in the partnership and one or more of the other computers in the
8 partnership store backup data received from the first computer; and
9 each of the computers in the partnership periodically verifying that its
10 backup data is being retained by one or more of the other computers in the
11 partnership.

1 50. (Previously Presented) The method according to claim 49, wherein the
2 verifying includes selecting a block of the previously backed up data wherein the
3 selecting is controlled by at least two of the computers.

1 51. (Previously Presented) The method according to claim 49, wherein the
2 partnership consists of two computers.

1 52. (Previously Presented) Computer readable media having stored thereon
2 computer code for a method of backing up data on a plurality of computers
3 connected via a network, the method comprising steps of:
4 exchanging messages among computers of the plurality to determine the
5 ability of each to satisfy backup storage requirements of one or more others;
6 forming a partnership among computers of the plurality in which a first
7 computer in the partnership stores backup data received from one or more other
8 computers in the partnership and one or more of the other computers in the
9 partnership store backup data received from the first computer; and

Atty. Dkt. No. 200301736-2

10 periodically verifying that stored backup data is being retained by one or
11 more of the computers in the partnership.

1 53. (Previously Presented) The method according to claim 1, wherein said
2 forming comprises forming at least two partnerships among the plurality of
3 computers.

1 54. (Previously Presented) The method according to claim 1, wherein at least
2 one computer of the plurality assumes the task of storing backup data received
3 from at least two other computers.

1 55. (Previously Presented) The method according to claim 1, wherein different
2 portions of data of at least one computer of the plurality are stored by at least two
3 other computers.

1 56. (Previously Presented) The method according to claim 49, further
2 comprising at least one additional partnership among the plurality of computers.

1 57. (Previously Presented) The method according to claim 49, wherein the first
2 computer of the partnership stores backup data received from at least two other
3 computers in the partnership.

1 58. (Previously Presented) The method according to claim 49, wherein different
2 portions of data of the first computer of the plurality are stored by at least two
3 other computers in the partnership.